



Intelligence

INTELLIGENCE SUPPORT TO THE AIR FORCE ACQUISITION PROCESS

This instruction implements AFRD 14-2, *Intelligence Collection, Production, and Application*, by providing guidance in identifying and acquiring intelligence to support the Air Force requirements and acquisition process. This AFI applies to all Air Force organizations and provides support beginning with Pre-Milestone 0 (pre MS-0) and continuing throughout the life cycle of a program, from identification of need through development, acquisition, testing, operational employment, and sustainment and modification. This instruction supports Defense Intelligence Agency (DIA) Regulation 55-3, *Intelligence Support for Defense Acquisition Programs*, March 30, 1992; DoD Instruction 5000.2/Air Force Supplement 1, *Defense Acquisition Management Policies and Procedures*, February 23, 1991, with Change 1; AFRD 10-6, *Mission Needs and Operational Requirements*; AFRD 62-2, *System Survivability*; AFRD 63-1, *Acquisition System*; and AFRD 99-1, *Test and Evaluation Process*. Attachment 1 lists the references, abbreviations, acronyms, and terms used.

SUMMARY OF CHANGES

This issuance aligns the instruction with AFRD 14-2.

Paragraph

Chapter 1--Responsibilities

HQ USAF/INXA	1.1
HQ 497th IG/INAA	1.2
Operating Commands	1.3
Implementing Command	1.4
Air Force Operational Test and Evaluation Center (AFOTEC).....	1.5

Chapter 2--Threat Support

Section A--Threat Support for the Weapon Systems Acquisition Process

Threat Support Process	2.1
Assessing Threats	2.2
Classifying Threat Assessments	2.3
Accrediting Threat Models	2.4

Section B--Supporting Pre-Milestone 0

Defining the Threat in MNSs.....	2.5
Reviewing and Approving MNSs.....	2.6

Section C--Supporting Milestone 0 to Milestone I

Program Initiation	2.7
Developing Documentation.....	2.8
Approval Authority.....	2.9
Getting Additional Milestone 0 to Milestone I Support	2.10

Section D--Supporting Post-Milestone I

Updating the COEA, ORD, and TEMP	2.11
Updating and Reviewing the STAR	2.12
Further Supporting Post-Milestone I	2.13

Supersedes AFR 200-13, 11 July 1990.
OPR: HQ AIA/DOA (Capt Mitch Matheys)

Certified by: HQ USAF/INXA (Mr Dennis M. Ring)
Pages: 16/Distribution: F

Chapter 3--Intelligence Infrastructure Support

Intelligence Infrastructure Support Process	3.1
Supporting Pre-Milestone 0	3.2
Supporting Milestone 0 to Milestone I	3.3
Supporting Post-Milestone I.....	3.4

Figures**Page**

2.1. Sample Threat Matrix.....	6
3.1. Potential ISWG Membership.....	8
3.2. Intelligence Tasks During the Requirements and Acquisition Process	9
3.3. ISP Development	10

Attachments

1. Glossary of References, Abbreviations, Acronyms, and Terms	11
2. System Threat Assessment Report (STAR) Format	15
3. Intelligence Support Plan Format.....	16

Chapter 1**RESPONSIBILITIES****1.1. HQ USAF/INXA:**

- 1.1.1. Provides policy and oversight on intelligence support to the acquisition and requirements processes.
- 1.1.2. Manages intelligence infrastructure support to Air Force acquisition programs for HQ USAF/IN:

- Assigns Intelligence Counterpart Officers (ICO) to all HQ USAF/XO and SAF/AQ designated programs.
- Reviews all Mission Need Statements (MNS) to assess intelligence infrastructure support requirements.
- Reviews all Operational Requirement Documents (ORD) to ensure they document adequate C3I infrastructure requirements.
- Cochairs Intelligence Support Working Groups (ISWG).
- Reviews draft Program Management Directives (PMD) during the preparation and updating cycle to ensure intelligence infrastructure support is properly tasked.
- Reviews and provides advice on intelligence infrastructure to the Cost and Operational Effectiveness Analysis (COEA).
- Reviews the sections of the Test and Evaluation Master Plan (TEMP) that relate to intelligence infrastructure.
- Provides critical intelligence infrastructure inputs for 497 IG/INAA to incorporate into the Air Force Systems Acquisition Review

Council (AFSARC) intelligence report.

- Coordinates with national intelligence organizations on intelligence support to acquisition.
- Reviews and recommends approval of Intelligence Support Plans (ISP) to HQ USAF/IN.

1.2. HQ 497th IG/INAA:

1.2.1. Manages threat support to Air Force acquisition programs for HQ USAF/IN.

1.2.1.1. Reviews and approves System Threat Assessment Reports (STAR) and System Threat Assessments (STA).

1.2.1.2. Reviews and approves the threat-related sections of:

- MNSs.
- COEAs.
- ORDs.
- TEMPs.

1.2.1.3. Reviews draft PMDs during preparation and updating to ensure threat support is properly assigned.

1.2.1.4. Prepares intelligence reports for the AFSARC documenting threats to the system and including intelligence support requirements at each milestone.

1.2.1.5. Prepares intelligence reports to support summits and similar service program reviews.

1.2.1.6. Chairs Threat Steering Groups (TSG) and participates in Threat Working Groups (TWG).

1.2.2. Performs threat model accreditation for AF

intelligence and weapon systems acquisition programs.

1.2.2.1. Chairs Threat Model Accreditation Working Groups (TMAWG).

1.3. Operating Commands:

1.3.1. Cochair Intelligence Support Working Groups (ISWG).

1.3.2. Prepare threat assessments in ORDs, COEAs, and MNSs.

1.3.3. Participate in STAR/STA TSGs and review STAR/STA drafts.

1.3.4. Fund tailored threat products that exceed the requirements for a STAR/STA.

1.3.5. In conjunction with HQ USAF/IN, recommend programs to be designated ICO/Intelligence Support Plan (ISP) programs.

1.3.6. Assign ICOs for HQ USAF/XO- or SAF/AQ-1.3.7. Conduct strategies-to-task analyses to determine intelligence infrastructure for all programs.

1.3.8. Develop ISPs for HQ USAF/XO- and SAF/AQ-selected acquisition programs.

1.3.9. Update ISPs annually and make them available 90 days before each milestone decision.

1.3.10. Program intelligence support resources required to satisfy unique weapon systems needs.

1.3.11. Generate intelligence collection, production, and systems requirements for the operational use of weapon systems.

1.3.12. Develop intelligence infrastructure requirements for ORDs, COEAs, TEMPs, and Integrated Weapon System Master Plans (IWSMP).

1.4. Implementing Command:

1.4.1. Provides threat and intelligence infrastructure support to research, development, test, acquisition, and sustainment activities.

1.4.1.1. Develops statements of intelligence requirements for collection, production, and infrastructure to research, develop, test, acquire, and maintain Air Force weapon systems and all major defense acquisition programs, including highly sensitive classified programs.

1.4.1.2. Provides tailored threat support to lab activities, Technical Planning Integrated Product Teams (TPIPT), development planners, and other pre-MS 0 activities.

1.4.2. Prepares STARS, STAs, threat assessments for TEMPs and Operational Test Plans (OTPs), and other threat-tailored documentation, as required.

1.4.3. Participates in TSGs, TWGs and ISWGs.

1.4.4. Provides routine intelligence support, review of Security Classification Guides, and contractor-release approval.

1.4.5. Prepares and submits Intelligence Production Requirements (IPR) and Statements of Intelligence Interest (SII).

1.4.6. Maintains threat documentation libraries.

1.5. Air Force Operational Test and Evaluation Center (AFOTEC):

1.5.1. Participates in ISWGs and TSGs.

1.5.2. Identifies and documents infrastructure support requirements for Operational Test and Evaluation (OT&E).

Chapter 2

THREAT SUPPORT

Section A--Threat Support for the Weapon Systems Acquisition Process

2.1. Threat Support Process:

2.1.1. **Purpose of Threat Support.** Accurate and timely threat support is needed to assess operational needs, prioritize new programs, and continually define a system during the acquisition process. Threat support includes threat assessment and threat model accreditation. HQ 497 IG/INAA manages threat support to Air Force acquisition programs for HQ USAF/IN.

2.2. **Assessing Threats.** Threat assessments support the systems acquisition, planning, programming, and budgeting process. They assess the potential of hostile parties to neutralize or degrade a specific US system. HQ 497 IG/INAA manages three primary categories of threat assessments in direct support of acquisition programs.

2.2.1. STARS and STAs:

2.2.1.1. The STAR is the authoritative, classified reference for Acquisition Category (ACAT) IC and ID programs. It:

- Describes in a concise, issue-oriented manner the lethal and nonlethal threats against the proposed US system and the threat environment in which the system will operate.
- Includes internal appendices (or separate supplements, if required) of detailed technical data, alternative scenarios (when applicable), and supporting analyses.
- Is based on the Defense Planning Guidance (DPG) scenarios, which give a broad overview of the expected threat environment and potential adversaries.

2.2.1.2. The (classified) STA is shorter (approximately 25 pages) and serves the ACAT II program. It follows the same format as the STAR (see attachment 2).

2.2.1.3. The system threat assessment for ACAT III-IV programs is the three- to five-page threat section in the ORD. In some non-warfighting systems the threat may be listed as not applicable. STARS and STAs are classified reports.

2.2.2. **Threat Environment Descriptions (TED).** TEDs are baseline threat documents that HQ 497 IG/INAA uses to support:

- All planning, programming, budgeting, development, and test and evaluation activities throughout the acquisition process.
- US Air Force mission areas and other specialized tasks, as AFM 1-1, volumes 1 and 2, *Basic Aerospace Doctrine of the US Air Force*, specify.
- Pre-Milestone I analyses.
- Programs not subject to the AFSARC and DAB milestone review process.
- STARS by addressing an entire Air Force mission area with greater breadth and scope than is usually found in STARS.
- ACAT III-IV programs that do not have an ORD.

NOTE: TEDs might also serve as an initial basis from which to develop a STAR.

2.2.2.1. National Air Intelligence Center (NAIC) produces TEDs biannually (with change pages to maintain currency) under the DoD Scientific and Technical Intelligence Production Program, which DIA monitors.

2.2.2.2. HQ USAF/IN approves TEDs and DIA validates them.

2.2.2.3. HQ 497 IG/INAA chairs Threat Steering Groups (TSGs), which plan the production and review of TEDs. Other participants include representatives from DIA, HQ AFMC, NAIC, and the intelligence staff of the appropriate operating commands.

2.2.3. **Intelligence Reports.** Intelligence Reports are concise, issue-oriented memorandums that HQ 497 IG/INAA:

- Prepares for HQ USAF/IN signature to support AFSARCs, summits, and other program reviews.
- Provides to the AFSARC secretary and SAF/AQ staff at least 5 days prior to the AFSARC.
- Distributes to AFSARC principals to address significant intelligence issues and to provide the HQ USAF/IN position regarding threat to the program.

2.2.3.1. Upon request from HQ USAF/XOR, HQ 497 IG/INAA prepares intelligence reports for ACAT II-IV programs.

2.2.4. **Threat Assessments in Other Documents.** ORDs, COEAs, and TEMPs all contain threat assessments. The threat data in these documents must

derive from and be consistent with the STAR/STA, TED, or DIA-validated information (when the STAR, STA, or TED is not available).

2.2.5. **Other Threat Documents.** Air Force MAJCOMs and units produce many of their own generic and program-specific threat documents. Upon request, HQ 497 IG/INAA provides broad guidance, helps incorporate material from relevant documents that other units of the intelligence community have previously produced, and reviews and approves finished products.

2.3. **Classifying Threat Assessments.** Threat assessments must be:

- Releasable to contractors.
- At the lowest possible classification consistent with user needs and security considerations.

For some programs, creators of threat assessment documents might need to prepare a separate annex at a higher classification level. **NOTE:** Highly sensitive, classified programs might require special-access STARS or, in some cases, STARS with special-access annexes.

2.4. **Accrediting Threat Models.** Accreditation is an official determination that a model is acceptable for a specific purpose. Accreditations can increase the level of credibility that threat models convey at the various review milestones.

2.4.1. Threat model accreditations are performed to support all phases of system acquisition, planning, programming, budgeting, and test and evaluation.

2.4.2. **Threat Model Accreditation Working Group (TMAWG) Accrediting.** The TMAWG is a team of experts assembled by HQ 497 IG/INAA to perform threat model accreditations, and includes the model's:

- Users.
- Beta site testers.
- Developers.
- Configuration control monitors.
- Analysts.
- System operators.

2.4.2.1. The TMAWG must act as an "honest broker" during the accreditation process by removing all organization agendas and providing a fair and honest appraisal of a model's capability to represent threat data accurately.

2.4.3. **Accrediting Computer Models.** Perform a computer model accreditation only after the developer or an independent agency completes verification and validation (V&V).

Section B--Supporting Pre-Milestone 0

2.5. **Defining the Threat in MNSs.** The operating MAJCOM prepares the initial threat assessment using DIA-approved threat information (such as Threat

Environment Descriptions). This threat analysis describes:

- The actual threat requiring an Air Force response.
- The projected threat environment.

2.5.1. MNS drafters may seek assistance from HQ 497 IG/INAA or local intelligence staffs to ensure that threat statements are consistent with current assessments.

2.6. Reviewing and Approving MNSs. HQ 497 IG/INAA reviews all MNSs to ensure that they are consistent with intelligence estimates and grants HQ USAF/IN approval of threat content.

Section C--Supporting Milestone 0 to Milestone I

2.7. Program Initiation. During the PMD preparation process, the staff of the Assistant Secretary for Acquisition (SAF/AQ) coordinates the draft PMD with HQ 497 IG/INAA to ensure threat support receives proper tasking. At Milestone 0 and subsequent milestones, HQ 497 IG/INAA prepares an intelligence report for the AFSARC documenting the threat to the system.

2.8. Developing Documentation. HQ 497 IG/INAA chairs a threat steering group that assists in drafting the initial STAR or STA.

2.8.1. Developing the COEA:

2.8.1.1. The threat analysis portion of the COEA:

- References the STAR.
- Describes projected enemy forces and tactics, including potential countermeasures.
- Describes the strengths and weaknesses of potential adversaries in the designated mission area and shows how these might change over time.

2.8.1.2. Base the scenarios used in the COEA on the DPG. Specifically, they should share underlying assumptions concerning the threat. The COEA drafter may consider when they would contribute to the analysis. In these instances, the COEA drafter clearly identifies and addresses any variance from the DPG scenario.

2.8.1.3. HQ 497 IG/INAA reviews and approves the intelligence-related sections of the COEA. As part of this review process, HQ 497 IG/INAA performs COEA data audits that:

- Verify the accuracy of the threat data in the model.
- Determine, to the extent possible, a level of confidence in the model.

2.8.2. Developing the ORD:

2.8.2.1. Programs that are threat-driven or that operate in a hostile environment must provide an ORD threat assessment. When a STAR or a stand-alone STA is available, the ORD references it and may incorporate its executive summary or portions of it into the ORD. When neither is available, the operating command prepares a three- to five-page threat assessment for the ORD that becomes the STA for that system.

2.8.2.2. The ORD threat assessment:

- Concisely describes the threat requiring an Air Force response and the projected threat environment in which the system will operate.
- Contains the following sections:
 - Operational threat environment.
 - System-specific threats at IOC and IOC + 10.
 - Targets (if applicable).
 - Reactive threat.

2.8.2.3. HQ 497 IG/INAA reviews and approves the threat section of the ORD.

2.8.3. Developing the TEMP:

2.8.3.1. The threat section of the TEMP:

- References the STAR.
- Briefly summarizes the threat environment described in the STAR. **EXCEPTION:** When the TEMP is required before formal program initiation (Milestone I) and no STAR/STA exists, the TEMP drafter will use threat information consistent with DIA- and HQ USAF/IN-approved intelligence.
- Identifies the type, number, availability, and fidelity requirements for all threat systems simulators.
- Compares the requirements for threat systems simulators with available and projected assets and their capabilities.
- Highlights major shortcomings.

2.8.3.2. HQ 497 IG/INAA reviews and approves the threat-related sections of the TEMP.

2.8.4. Developing the STAR/STA:

2.8.4.1. A STAR or stand-alone STA is prepared for ACAT I and II programs and others as required. Developing a STAR requires the formation of a threat steering group (TSG). The TSG acts as an advisory body on threat matters. HQ 497 IG/INAA determines within 30 days of the initial PMD date whether a TSG must support a program.

2.8.4.2. HQ 497 IG/INAA chairs the TSG, which may include:

- Representatives from HQ 497 IG/INAA.
- Service intelligence agencies (for joint programs).
- Intelligence staff of the implementing and

- operating commands.
- The originating office of the STAR.
- System program office (SPO) staff.
- SAF/AQ staff.
- DIA (for DAB programs).
- NAIC.
- AFOTEC, when operational test and evaluation become an issue.
- Others as appropriate.

2.8.4.3. TSG responsibilities include:

- Scheduling STAR production.
- Establishing tasking.
- Determining requirements for exceptional documents, such as STAR supplements.
- Drafting a threat matrix according to the format in figure 2.1.
 - Preparing a STAR outline.
 - Advising on critical intelligence parameters (CIP) development.

THREATS TO (US SYSTEM) (U)

THREAT	IOC	IOC+10
Threat A	High	High
Threat B	Low	Nil
Threat C	Nil	Medium
Threat D	Medium	High

Figure 2.1. Sample Threat Matrix.

2.9. Approval Authority:

2.9.1. HQ USAF/IN grants approval of threat assessments for ACAT IC (except at Milestone I) and ACAT II programs.

2.9.2. HQ USAF/IN grants Air Force approval for ACAT IC (at Milestone I) and ACAT ID programs before they are submitted to DIA for validation.

2.10. Getting Additional Milestone 0 to Milestone I Support. In some instances, additional threat support is needed before formal program initiation (Milestone I). Intelligence provided before Milestone I must:

- Be consistent with DIA- and HQ USAF/IN-approved intelligence.
- Contain a statement explaining the purpose of the document.

Section D--Supporting Post-Milestone I

2.11. Updating the COEA, ORD, and TEMP. The operating MAJCOM updates threat data in the COEA and ORD for subsequent milestone reviews. The implementing command updates threat data in the TEMP.

2.12. Updating and Reviewing the STAR:

2.12.1. About 6 weeks before the anniversary of a STAR, HQ 497 IG/INAA requests general review and recommends whether the STAR needs an update from DIA, the implementing or operating commands, or NAIC.

2.12.2. The reviewers send their recommendations to HQ 497 IG/INAA, with information copies to the implementing command and the STAR originator, within 21 days following the request for review.

2.12.3. On or before the anniversary date, HQ 497 IG/INAA decides whether the STAR requires updating.

2.12.4. If the STAR does not require updating, HQ 497 IG/INAA will obtain the concurrence of the intelligence

staffs of the implementing and operating commands. The STAR originator will prepare a letter for distribution with attachments (as a minimum, a new preface page).

2.12.5. If HQ 497 IG/INAA decides that the STAR requires updating, it will then decide whether to convene a TSG. **NOTE:** HQ 497 IG/INAA requests a TSG when the potential changes are great enough to warrant it or when it is not sure if the changes in a threat warrant a change to the STAR.

2.12.6. The STAR originator updates the document (or appropriate portions of the document).

2.12.7. Not later than 90 days after the STAR's anniversary, the STAR originator sends copies of the update for comment to NAIC, the intelligence staffs of the implementing and operating commands, and HQ 497 IG/INAA.

2.12.8. The operating command and NAIC submit comments to HQ 497 IG/INAA within 30 calendar days after receiving the draft STAR.

2.12.9. HQ 497 IG/INAA sends the STAR originator a set of integrated comments and a letter of approval within 21 calendar days. **NOTE:** When HQ USAF/IN has approved the changes, the following statement is placed in the preface: "This document has been reviewed by HQ USAF/IN and is approved for use in support of the (program title) program as of (publication date) and is effective through (18 months) unless earlier superseded."

2.12.10. HQ 497 IG/INAA provides copies of the draft STAR to the appropriate sister services and asks for

review comments in support of joint programs within 45 days.

2.12.11. HQ 497 IG/INAA incorporates these comments in a response to the STAR originator, noting the extent of review and coordination on the preface page of the STAR.

2.12.12. According to DIAR 55-3, HQ 497 IG/INAA submits STARs for ACAT ID (and ACAT IC at Milestone I) programs to DIA for validation.

2.12.13. Once a STAR or related document has entered the intelligence review cycle, agencies participating in that review will not distribute the draft to other agencies until after final approval and validation. HQ 497 IG/INAA may waive this restriction.

2.12.14. After a STAR has been approved and validated, the STAR originator produces interim changes or revisions when significant changes occur in either the threat or the US system specifications and characteristics.

2.12.15. Stand-alone STAs and STAR supplements follow the same review procedures as STARs.

2.12.16. After Milestone III, STARs/STAs and threat assessments in other documents are updated and refined on an "as required" basis.

2.13. Further Supporting Post-Milestone I. The implementing command provides required threat support throughout the system development and testing process.

2.13.1. When extraordinary threat support or documentation (other than the STAR) is required, the program director allocates resources to the intelligence producer as necessary.

Chapter 3

INTELLIGENCE INFRASTRUCTURE SUPPORT

3.1. Intelligence Infrastructure Support Process:

3.1.1. **Managing Intelligence Infrastructure Support.** HQ USAF/INXA manages intelligence infrastructure support to Air Force acquisition programs for HQ USAF/IN.

3.1.2. **Creating the Intelligence Support Plan (ISP).** The ISP (see attachment 3) is the authoritative reference for intelligence infrastructure support to a specific weapon system. The ISP documents and facilitates interaction and agreement between those who acquire and operate weapon systems (including testing and training) and those who provide its intelligence support. DoD Instruction 5000.2/Air Force Supplement 1 and DoD 5000.2-M, *Defense Acquisition Management Documentation and Reports*, February 1991, is the authority for the ISP.

3.1.2.1. A program's PMD states whether the ICO must develop an ISP.

3.1.2.2. When an ISP is not available, follow the intelligence infrastructure requirements in the ORDs.

3.1.2.3. The ISP addresses, at a minimum, all requirements for weapon system, life-cycle intelligence support related to:

- Collection management.
- Tailored threat production.
- Collection, exploitation, and production of multidisciplined, fused intelligence.
- Intelligence dissemination.
- Intelligence manpower and training.
- Targeting intelligence.
- Mapping, charting, and geodesy (MC&G).
- Combat intelligence data.
- Modeling and simulation.

- Simulator validation (SIMVAL).
- Foreign material exploitation and military sales.

3.1.3. **Getting Help With the ISP From the Intelligence Counterpart Officer (ICO).** The ICO is the single staff focal point for intelligence infrastructure support to a specific weapon system or a class of weapon systems. ICOs identify, budget for, and coordinate all intelligence support requirements for weapon systems.

3.1.3.1. The ICO develops and coordinates systems-specific ISPs to document and implement mutually agreed-upon intelligence support requirements.

3.1.3.1.1. The operating command ICO leads development of the ISP, while the FOA ICO helps produce the ISP by advising on requirements and costs to

the Air Force and national intelligence community.

3.1.4. **The Intelligence Support Working Group (ISWG).** The ISWG helps the operating command ICO put together the ISP and monitors ISP execution and revision throughout the system's life cycle. The ISWG includes five major interest groups:

- System developers and supporters.
- System testers.
- Operational users.
- Supporting intelligence providers.
- Those responsible for intelligence support training.

3.1.4.1. The operating command and HQ USAF/INXA cochair the ISWG. Figure 3.1 lists some of the key organizations that typically attend the ISWG.

INTEREST GROUPS	ORGANIZATIONS
Developers/Supporters	AFMC/XR Weapon System SPO ESC/AMC/SMC/HSC Operating Command(s) Requirements Staff Reps AF/XOR SAF/AQ AF/PEO Staff Other Services and Joint Representatives
Testers	Air Force Operational Test and Evaluation Center (AFOTEC) AF/TEP Responsible Test Organizations and Labs
Operators	AF/XOF/XOO Operating Command DO Reps Other Services and Joint Representatives
Intelligence Providers	HQ 497 IG AF/INX Product Center Directors of Intelligence Operating Command(s) ICO(s) and IN Staff Reps Defense Intelligence Agency (DIA) Defense Mapping Agency (DMA) Air Intelligence Group (AIG) Representative Joint Intelligence Center (JIC) Representative Air Intelligence Agency (AIA)
Trainers	Air Education and Training Command (AETC) AF/INR
Others	TENCAP Representatives Selected Contractors

Figure 3.1. Potential ISWG Membership.

3.1.5. **Developing the ISP.** The operating command ICO:

- Develops the ISP in close cooperation with the Air Force operational, acquisition, intelligence, and test communities.
- Signs and submits the ISP to the Director of Operations and the Director of Requirements at the using command, as well as to the SPO Director.

- Sends the signed ISP to HQ USAF/INXA for Air Staff coordination before HQ USAF/IN grants final approval.

3.1.6. **Updating the ISP.** About 6 weeks before the publication anniversary of an ISP, HQ USAF/INXA requests general review of and recommendations on the need for an update from the operating command.

3.1.6.1. If the ISP does not require updating, the operating command prepares and distributes a letter with

attachments (at least, a new preface page) for inclusion in the ISP.

3.1.7. Placing the ISP in Context. Figure 3.2 places the ISP within the context of the requirements and acquisition process. Figure 3.3 places the ISP within the context of the overall analytical process used to determine intelligence support requirements. Formal drafting of the ISP begins immediately after Milestone 0.

3.1.8. Classifying ISPs. ISPs must be:

- Releasable to contractors.
- At the lowest possible classification consistent with user needs and security considerations.

3.1.8.1. For some programs, creators of ISPs might need to prepare a separate annex at a higher classification level or one that is not releasable to contractors. **NOTE:** Highly sensitive classified programs might require

special-access ISPs or, in some cases, ISPs with special-access annexes.

3.2. Supporting Pre-Milestone 0:

3.2.1. During its initial planning, the operating command assigns an ICO to provide input to and review of the MNS.

3.2.2. The operating command ICO conducts a Strategy-To-Task (STT) analysis.

3.2.3. When the MNS reaches HQ USAF/INX during the "for comment" coordination phase, HQ USAF/IN assigns an ICO to survey Air Force intelligence support needs.

3.2.4. The HQ USAF/INXA ICO documents the issues that this survey presents, coordinates resources as necessary, and starts validating the intelligence infrastructure requirements.

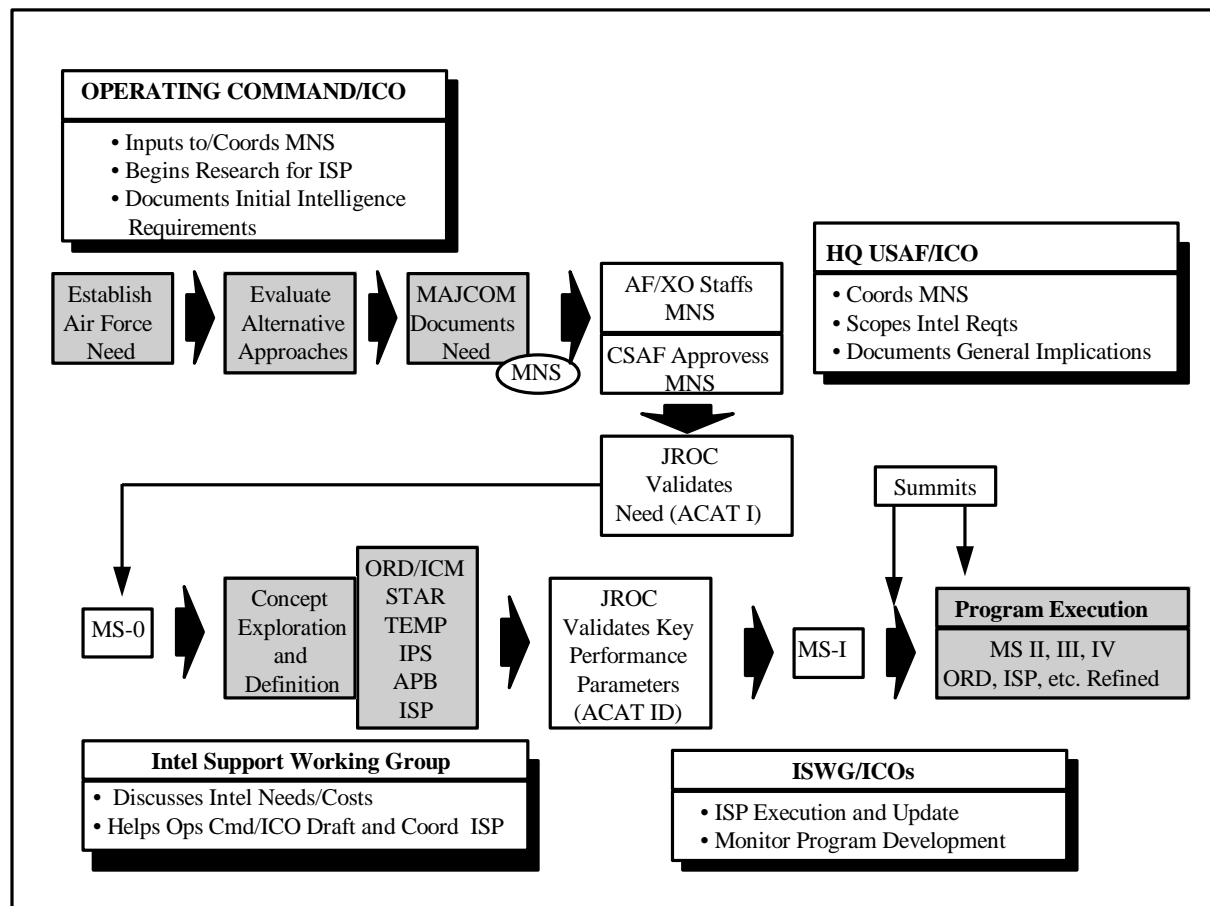


Figure 3.2. Intelligence Tasks During the Requirements and Acquisition Process.

3.2.5. During this period, the implementing agencies (Technical Planning Integrated Product Teams [TPIPT], requirements staffs, Center/Lab/MAJCOM IN, SPO, and so forth) provide tentative acquisition and sustainment requirements for intelligence support.

3.2.6. The ICO translates these tentative requirements into intelligence requirements and identifies shortcomings and corrective actions.

3.3. Supporting Milestone 0 to Milestone I:

3.3.1. HQ USAF/INXA and the using command, together with functional experts from other commands and organizations, form an ISWG for HQ USAF/XO and SAF/AQ programs immediately after Milestone 0.

3.3.2. The ISWG helps the using command put together the Intelligence Support Plan (ISP), using functional area checklists to ensure accuracy and completeness.

3.3.3. ISWG inputs are put into the Cost and Operational Effectiveness Analysis (COEA) as part of the projected life-cycle cost for a given program.

3.4. Supporting Post-Milestone I:

3.4.1. The ISWG and ICOs refine requirements and monitor ISP progress throughout the weapon system's life cycle.

3.4.2. ICOs participate in summits, design reviews, test working groups, and other program management forums to monitor overall intelligence support and ensure that ISP requirements are satisfied.

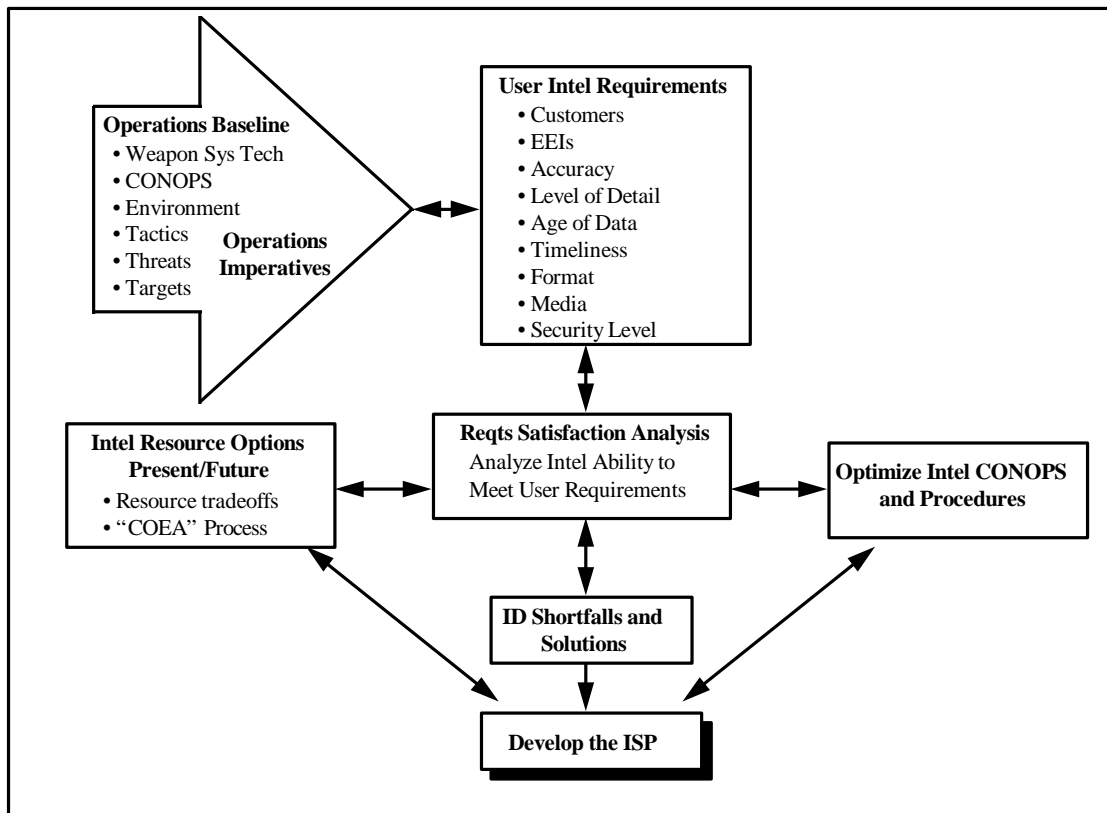


Figure 3.3. ISP Development.

ERVIN J. ROKKE, Maj General, USAF
Assistant Chief of Staff, Intelligence

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS***Section A--References***

NOTE: The user of this instruction should verify the currency of the cited documents.

DIAR 55-3, *Intelligence Support for Defense Acquisition Programs*, March 30, 1992

DoD Instruction 5000.2/Air Force Supplement 1, *Defense Acquisition Management Policies and Procedures*, February 23, 1991, with Change 1

AFPD 10-6, *Mission Needs and Operational Requirements*

AFPD 14-2, *Intelligence Collection, Production, and Application*

AFPD 62-2, *System Survivability*

AFPD 63-1, *Acquisition System*

AFPD 99-1, *Test and Evaluation Process*

Section B--Abbreviations and Acronyms***Abbreviations
and Acronyms******Definitions***

ACAT	Acquisition Category
AFPD	Air Force Policy Directive
AFSARC	Air Force Systems Acquisition Review Council
APB	Acquisition Program Baseline
C ³ I	Command, Control, Communications, and Intelligence
COEA	Cost and Operational Effectiveness Analysis
DAB	Defense Acquisition Board
DIA	Defense Intelligence Agency
DPG	Defense Planning Guidance
FOA	Field Operating Agency
ICO	Intelligence Counterpart Officer
IOC	Initial Operational Capability
IPR	Intelligence Production Requirement
IPS	Integrated Program Summary
ISP	Intelligence Support Plan
ISWG	Intelligence Support Working Group

IWSMP	Integrated Weapon System Master Plan
JROC	Joint Requirements Oversight Council
MNS	Mission Need Statement
MS	Milestone
ORD	Operational Requirement Document
OT&E	Operational Test and Evaluation
OTP	Operational Test Plan
PMD	Program Management Directive
SII	Statement of Intelligence Interest
SPO	System Program Office
STA	System Threat Assessment
STAR	System Threat Assessment Report
STT	Strategy-To-Task
TED	Threat Environment Description
TEMP	Test and Evaluation Master Plan
TMAWG	Threat Model Accreditation Working Group
TIPT	Technical Planning Integrated Product Team
TSG	Threat Steering Group
TWG	Threat Working Group
V&V	Verification and Validation

Section C--Terms

NOTE: See Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 1 May 1988, and AFM 11-1, *Air Force Glossary of Standard Terms*, for other standardized terms and definitions.

Acquisition Categories (ACAT)--Categories set up to decentralize decision-making and to execute and comply with statutory requirements. The categories determine the level of review, decision authority, and applicable procedures (AFPD 63-1). There are four program categories, which derive from research, development, test and evaluation (RDT&E) or procurement costs (in FY 90\$):

ID: \$300 million RDT&E or \$1.8 billion procurement and production (Office of Secretary of Defense approval).

IC: \$300 million RDT&E or \$1.8 billion procurement and production (Service approval).

IM: \$100 million program cost (ASD/C³I approval).

II: \$115 million RDT&E or \$540 million procurement and production.

III: Less than above, but designated III by Service Acquisition Executive (SAE).

IV: All other programs.

(DoD Instruction 5000.2/Air Force Supplement 1)

Acquisition Decision Memorandum (ADM)--A memorandum signed by the milestone decision authority documenting the decisions made and the exit criteria set up as a result of a milestone decision review or an in-process review. (DoD Instruction 5000.2/Air Force Supplement 1)

Air Force Systems Acquisition Review Council (AFSARC)--The Air Force corporate body that advises the Air Force acquisition executive on the initiating, continuing, or substantially changing major defense acquisition programs. (AFPD 63-1)

Concept Studies--Studies conducted to evaluate and define the feasibility of alternative concepts. They assess the relative merits of alternative concepts at the Milestone I decision point. (AFI 10-601)

Cost and Operational Effectiveness Analysis (COEA)--An analysis of the estimated costs and operational effectiveness of alternative materiel systems to meet a mission need and the associated program for acquiring each alternative. (DoD Instruction 5000.2/Air Force Supplement 1)

Critical Intelligence Parameters (CIP)--A threat capability or threshold set by the program, changes to which could critically impact the effectiveness and survivability of the proposed system. (AFI 10-601)

Defense Acquisition Board (DAB)--The Department of Defense corporate body for system acquisition that advises and assists the Secretary of Defense. (DoD Directive 5000.49)

Defense Planning Guidance (DPG)--Secretary of Defense's policy and fiscal guidance upon which the military services and defense agencies base their progress and budgets. The DPG provides a broad overview of the expected threat environment and potential adversaries. To establish a thread of continuity in Air Force system threat assessment reports (STAR), DPG scenarios will form the basis for the operation threat environments in STARS.

Implementing Command--The command or agency that the Air Force Acquisition Executive designates to manage an acquisition program (DoD Instruction 5000.2/Air Force Supplement 1)

Milestones (O through IV)--Major management decision points in the overall acquisition decision process of a Department of Defense (DoD) system that requires Office of the Secretary of Defense and (or) DoD component program review. Milestones include both the Defense Acquisition Board and DoD component-equivalent program reviews: (AFI 10-601)

- 0 - Concept Studies Approval
- I - Concept Demonstration Approval
- II - Development Approval
- III - Production Approval
- IV - Major Modification Approval

Mission Need Statement (MNS)--A document that identifies a materiel requirement to satisfy a mission deficiency. (AFI 10-601)

Operating Command--The command primarily operating a system, subsystem, or item of equipment. Generally applies to those operational commands or organizations that Headquarters US Air Force designates to conduct or participate in operations or operational testing. Interchangeable with the term "Using Command." (AFM 11-1)

Operational Requirements Document (ORD)--A document prepared by the respective operating command that describes pertinent quantitative and qualitative performance, operation, and support parameters; characteristics; and requirements for a specific candidate weapon system. The ORD documents how users operate, deploy, employ, and support a system and provides initial guidance for the implementing, supporting, and participating commands and agencies. (AFI 10-601)

Program Management Directive (PMD)--The PMD directs the implementation of decision documentation in an acquisition decision memorandum--PMDs initiate and terminate actions, cite funding sources, and assign responsibilities and tasks to appropriate commands and agencies.

SYSTEM THREAT ASSESSMENT REPORT (STAR) FORMAT

A2.1. Preface. A formatted page outlining the scope of the STAR, the offices involved in preparation, the responsible program office, the information cutoff date, the milestone that it supports, the Air Force approval statement, and (if applicable) the DIA validation statement.

A2.2. Table of Contents and List of Figures and Illustrations.

A2.3. Executive Summary. The executive summary consists of three subsections:

- US Systems Description (with system IOC).
- Key Threat Judgments.
- A Threat Matrix.

It specifically identifies significant threat changes that have been noted since the last STAR.

A2.4. Section I. Introduction. A brief opening statement that includes a short description of the mission need for the system.

A2.5. Section II. US System Description. A summary that includes physical and technical characteristics, the IOC, mission, operational concepts, and employment considerations that can reasonably be expected to impact on, or be impacted by, the threat. The program office provides US System Description information. The operating command provides mission and concept of operations information.

A2.6. Section III. Operational Threat Environment. A generalized overview of the operational, physical, and technological environment in which the system is expected to operate during its lifetime. Areas covered include:

- Threat force levels and enemy doctrine.
- Strategy.
- Tactics affecting system mission and operations.

Scenarios in this section are based on the DPG scenarios.

A2.7. Section IV. Targets (if applicable). An analysis of the capabilities and signatures of the full range of targets (such as vehicles, ships, aircraft, or silos) the US system is designed to engage. Target employment, characteristics, command and control, and numbers are included. Types and density of targets may also be covered along with such common parameters as the thickness and types of armor the system must defeat.

A2.8. Section V. System Specific Threat. An assessment of the threats that are directly relevant to the mission and performance of the US system throughout its operational lifetime. This section consists of two subsections: the threat at IOC of the US system and the threat at IOC plus 10 years. Each subsection assesses the threat using three criteria:

- Description of the threat system.
- Magnitude of the threat (projected force level).
- Threat integration--a combined evaluation of the threat to the US system when a potential adversary's employment doctrine, force levels, and systems are considered together.

A2.9. Section VI. Reactive Threat. Summarizes both the likely reactive threat and the technologically feasible threat. The likely reactive threat describes the system or capabilities that adversaries most typically develop and deploy during a specified period. The technologically feasible threat offers alternatives if the adversary's requirements differ from those that intelligence sources have generated. Although not constrained by intelligence projections, the technologically feasible threat is consistent with an adversary's technology, economic, and production capabilities.

A2.10. Appendices. Appendix 1 lists the CIPs and associated IPRs. CIPs are developed for the initial STAR. Updates to the STAR focus on relevant intelligence. The CIP threat status is also provided along with each CIP. The system program office and the originating office of the STAR work together to develop CIPs. A new IPR is developed for each CIP in the STAR.

A2.11. References. A list that contains sources used in the preparation of the document.

INTELLIGENCE SUPPORT PLAN FORMAT

A3.1. Chapter 1. Introduction:

- a. **Section 1. Role of the ISP.** Overview, purpose of the ISP, and associated tasks.
- b. **Section 2. Understanding the Operations-Imperative Approach.** Overview, defining the operations-imperative approach, how the approach works, satisfaction criteria and values, and elements of satisfaction and values.
- c. **Section 3. How to Use This ISP.** Overview, ISP user information needs, organization of the ISP, intelligence support requirements matrix, derived intelligence support requirements, sources of the document, and intended users of the ISP.

A3.2. Chapter 2. Introduction to Acquisition and System Support:

- a. **Section 1. Weapon System.** Overview, description, missions and roles, top-level concerns, and understanding weapon system terminology.
- b. **Section 2. Process to Complete Mission Plan.** Overview and system tasks.
- c. **Section 3. Mission Requirements.**
- d. **Section 4. Operational Employment and Deployed Capability.**
- e. **Section 5. Support to Testing.**
- f. **Section 6. Training.** Overview, training concerns, training needed for acquisition testing, training skills for operational employment, and training data requirements.

A3.3. Chapter 3. Derived Intelligence Support Requirements:

- a. **Section 1. Intelligence Support Requirements Matrix.** Overview, status indicator symbols, and intelligence support requirements matrix.
- b. **Section 2. Derived Intelligence Support Requirements Overview.** Developing comprehensive CONOP, intelligence data requirements, target model validation, digital imagery exploitation support, mission planning, deployed capability, targeting in the theater of operations, targeting support for testing, mission assessment, national level support, and intelligence training program.

A3.4. Chapter 4. Proposed Intelligence Cost:

- a. **Section 1. Proposed Intelligence Support.** Overview, current intelligence support and capabilities, and proposed intelligence support and capabilities.
- b. **Section 2. Assumptions and Costs for Scenario #1.** Overview, Assumption #1 and cost estimate, and Assumption #2 and cost estimate.
- c. **Section 3. Assumptions and Costs for Scenario #2.** Overview, Assumption #3 and cost estimate, and Assumption #4 and cost estimate.

A3.5. Glossary.